

**IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF GEORGIA  
ATLANTA DIVISION**

JOSEPH D'ANGELO, III, SHAWN P. )  
HAGGERTY, CHARITY L. LATIMER, )  
KURT J. MCLAUGHLIN, TAMARA )  
NEDLOUF, and JOHN A. THOMAS, II, )  
 )  
Plaintiffs, )  
 )  
v. )  
 )  
ANTHEM, INC., and BLUE CROSS AND )  
BLUE SHIELD OF GEORGIA, INC. )  
 )  
Defendants. )

CIVIL ACTION

FILE NO. \_\_\_\_\_

**JURY DEMAND**

**COMPLAINT**

1. Unidentified hackers recently penetrated Anthem, Inc.'s computer network. The breach resulted in the hackers gaining access to a host of personal information for customers and employees, including Anthem's CEO, Joseph Swedish. Upon information and belief, hackers have gained access to the names, birthdates, email addresses, employment details, social security numbers, incomes, and street addresses of people who are currently covered or have been covered by Anthem's insurance policies. Given that Anthem is the nation's second largest health insurer, this breach is potentially one of the largest data breaches in the history of the world.

**PARTIES**

2. Plaintiff Joseph D'Angelo, III is a citizen of the state of Georgia.
3. Plaintiff Shawn P. Haggerty is a citizen of the state of Georgia.
4. Plaintiff Charity L. Latimer is a citizen of the state of Georgia.
5. Plaintiff Kurt J. McLaughlin is a citizen of the state of Georgia.
6. Plaintiff Tamara Nedlouf is a citizen of the state of Georgia.
7. Plaintiff John A. Thomas, II, is a citizen of the state of Georgia.
8. Defendant Anthem, Inc. ("Anthem") is one of the largest health benefits companies in the United States. Headquartered in Indianapolis, Indiana, Anthem is an independent licensee of the Blue Cross and Blue Shield Association serving members in California, Colorado, Connecticut, Georgia, Indiana, Kentucky, Maine, Missouri, Nevada, New Hampshire, New York, Ohio, Virginia, and Wisconsin, and specialty plan members in other states. Through its affiliated health plans, Anthem companies deliver a number of leading health benefit solutions through a broad portfolio of integrated health care plans and related services, along with a wide range of specialty products such as life and disability insurance benefits, dental, vision, behavioral health benefit services, as well as long term care insurance and flexible spending accounts.

9. Defendant Blue Cross and Blue Shield of Georgia, Inc. (“Blue Cross”) is an affiliate of Anthem that serves customers in the state of Georgia, including Plaintiffs. Blue Cross conceded that its customers were subject to the data breach in a notice sent on February 5, 2015, which stated as follows:

Safeguarding your personal, financial and medical information is one of our top priorities, and because of that, we have state-of-the-art information security systems to protect your data. However, despite our efforts, Blue Cross and Blue Shield of Georgia was the target of a very sophisticated external cyber attack. These attackers gained unauthorized access to Blue Cross and Blue Shield of Georgia’s IT system and have obtained personal information from our current and former members such as their names, birthdays, medical IDs/social security numbers, street addresses, email addresses and employment information, including income data. Based on what we know now, there is no evidence that credit card or medical information (such as claims, test results or diagnostic codes) were targeted or compromised.

Once the attack was discovered, Blue Cross and Blue Shield of Georgia immediately made every effort to close the security vulnerability, contacted the FBI and began fully cooperating with their investigation. Blue Cross and Blue Shield of Georgia has also retained Mandiant, one of the world’s leading cybersecurity firms, to evaluate our systems and identify solutions based on the evolving landscape.

Blue Cross and Blue Shield of Georgia’s own associates’ personal information – including my own – was accessed during this security breach. We join you in your concern and frustration, and I assure you that we are working around the clock to do everything we can to further secure your data.

Blue Cross and Blue Shield of Georgia will individually notify current and former members whose information has been accessed. We will provide credit monitoring and identity protection services free of

charge so that those who have been affected can have peace of mind. We have created a dedicated website - AnthemFacts.com - where members can access information such as frequent questions and answers. As we learn more, we will continually update this website and share that information with you. We have also established a dedicated toll-free number that both current and former members can call if they have questions related to this incident. That number is: 1-877-263-7995.

I want to personally apologize to each of you for what has happened, as I know you expect us to protect your information. We will continue to do everything in our power to make our systems and security processes better and more secure, and hope that we can earn back your trust and confidence in Blue Cross and Blue Shield of Georgia.

Sincerely,

Joseph Swedish  
President and CEO  
Anthem, Inc.

#### **JURISDICTION AND VENUE**

10. This Court has diversity jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). Some Plaintiffs and proposed class members and some Defendants are citizens of different states, the amount in controversy exceeds \$5,000,000.00, and there are more than 100 putative class members.

11. This Court has personal jurisdiction over Anthem and Blue Cross because they maintain places of business in Georgia, regularly conduct business in Georgia, and have sufficient minimum contacts in Georgia. Anthem and Blue

Cross intentionally avail themselves of this jurisdiction by marketing and selling health insurance to Georgia consumers.

12. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a) because Anthem and Blue Cross do business in this District and substantial events, acts, and omissions giving rise to Plaintiffs' claims occurred in this District.

### **COMMON FACTUAL ALLEGATIONS**

13. With nearly 69 million people served by its affiliated companies including more than 37 million enrolled in its family of health plans, Anthem is one of the nation's leading health benefits companies.

14. When consumers enroll in health insurance plans with Anthem, Defendants collect personal information related to the enrollment process, including but not limited to customers' names, birthdates, email addresses, employment details, social security numbers, incomes, and street addresses.

15. While Anthem's collection of customer information may itself be legal, by collecting and storing such extensive and detailed customer information, Anthem creates an obligation for itself to use every means available to it to protect this information from falling into the hands of identity thieves and other criminals.

16. Over at least the past several weeks, computer hackers have gained access to Anthem's data network. Personal information regarding tens of millions of consumers stored by Anthem has been compromised.

17. On February 4, 2015, the first public report of Anthem's data breach was made by several news outlets.

18. The personal and financial information of consumers, including Plaintiffs and the proposed Class members, is valuable.

19. The Federal Trade Commission ("FTC") warns consumers to pay particular attention to how they keep personally identifying information: Social Security numbers, credit card or financial information, and other sensitive data. As the FTC notes, "[t]hat's what thieves use most often to commit fraud or identity theft."

20. The information stolen from Anthem, including Plaintiffs' and Class members' personal and/or financial information, is extremely valuable to thieves. As the FTC recognizes, once identity thieves have personal information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."

21. Personal and financial information such as that stolen in the Anthem data breach is highly coveted by and a frequent target of hackers. Legitimate

organizations and the criminal underground alike recognize the value of such data. Otherwise, they would not pay for or maintain it, or aggressively seek it. Criminals seek personal and financial information of consumers because they can use biographical data to perpetuate more and larger thefts.

22. The ramifications of Anthem's failure to keep Plaintiffs' and Class members' personal and/or financial information secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, address, social security number, date of birth, and other information, without permission, to commit fraud or other crimes.

23. Identity thieves can use personal information such as that pertaining to Plaintiffs and the Class, which Anthem failed to keep secure, to perpetuate a variety of crimes that harm the victims. For instance, identity thieves may commit various types of crimes such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, using the victim's information to obtain government benefits, or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund. The United States government and privacy experts acknowledge that it may take years for identity theft to come to light and be detected.

24. This is not the first time that Anthem has failed to adequately protect the personal information of its customers. For example, between 2011 and 2012, Anthem illegally exposed over 30,000 customer social security numbers and ended up settling the matter with the California Attorney General.

25. In 2013, Defendant Anthem agreed to pay \$1.7 million to resolve allegations it left the information of more than 612,000 members available online because of inadequate safeguards.

26. The U.S. Department of Health and Human Services said that Defendant's security weaknesses in an online application database left names, birthdates, addresses, telephone numbers, Social Security numbers, and health data accessible to unauthorized users.

27. The Health and Human Services Department said then that Defendant Anthem did not have adequate policies for authorizing access to the database, did not perform a needed technical evaluation after a software upgrade, and did not have technical safeguards to verify that the people or entities seeking access were authorized to view the information in the database.

28. Health insurers are known to be targets of identity thieves. Indeed, on April 8, 2014, the FBI issued a warning to all healthcare providers. Unfortunately,

Anthem did not take such warnings seriously and its lax data safeguards have caused damage to its customers yet again.

### **PLAINTIFFS' FACTUAL ALLEGATIONS**

29. Plaintiff Joseph D'Angelo, III is a customer of Defendants. When becoming a customer of Defendants, he provided Defendants with sensitive personal and/or financial information. He reasonably believed Defendants would maintain this personal and/or financial information in a secure manner and provided his information to Defendants on that basis. Had he known that Defendants would not maintain his information in a reasonably secure manner, he would not have provided that information to Defendants.

30. Mr. D'Angelo's personal information was compromised in and as a result of the Anthem data breach. He was harmed by having his financial and/or personal information compromised and faces the imminent threat of future additional harm from the increased risk of identity theft and fraud due to his financial and/or personal information being sold on the Internet black market and/or misused by criminals.

31. Plaintiff Shawn P. Haggerty is a customer of Defendants. When becoming a customer of Defendants, he provided Defendants with sensitive personal and/or financial information. He reasonably believed Defendants would

maintain this personal and/or financial information in a secure manner and provided his information to Defendants on that basis. Had he known that Defendants would not maintain his information in a reasonably secure manner, he would not have provided that information to Defendants.

32. Mr. Haggerty's personal information was compromised in and as a result of the Anthem data breach. He was harmed by having his financial and/or personal information compromised and faces the imminent threat of future additional harm from the increased risk of identity theft and fraud due to his financial and/or personal information being sold on the Internet black market and/or misused by criminals.

33. Plaintiff Charity L. Latimer was a customer of Defendants until very recently. When becoming a customer of Defendants and thereafter, she provided Defendants with sensitive personal and/or financial information. She reasonably believed Defendants would maintain this personal and/or financial information in a secure manner and provided information to Defendants on that basis. Had she known that Defendants would not maintain the information in a reasonably secure manner, she would not have provided that information to Defendants.

34. Ms. Latimer's personal information was compromised in and as a result of the Anthem data breach. She was harmed by having her financial and/or

personal information compromised and faces the imminent threat of future additional harm from the increased risk of identity theft and fraud due to her financial and personal information being sold on the Internet black market and/or misused by criminals.

35. Plaintiff Mr. McLaughlin is a customer of Defendants. When becoming a customer of Defendants, he provided Defendants with sensitive personal and/or financial information. He reasonably believed Defendants would maintain this personal and/or financial information in a secure manner and provided his information to Defendants on that basis. Had he known that Defendants would not maintain his information in a reasonably secure manner, he would not have provided that information to Defendants.

36. Mr. McLaughlin's personal information was compromised in and as a result of the Anthem data breach. He was harmed by having his financial and/or personal information compromised and faces the imminent threat of future additional harm from the increased risk of identity theft and fraud due to his financial and/or personal information being sold on the Internet black market and/or misused by criminals.

37. Plaintiff Tamara Nedlouf is a customer of Defendants. When becoming a customer of Defendants and thereafter, she provided Defendants with

sensitive personal and/or financial information. She reasonably believed Defendants would maintain this personal and/or financial information in a secure manner and provided information to Defendants on that basis. Had she known that Defendants would not maintain the information in a reasonably secure manner, she would not have provided that information to Defendants.

38. Ms. Nedlouf's personal information was compromised in and as a result of the Anthem data breach. She was harmed by having her financial and/or personal information compromised and faces the imminent threat of future additional harm from the increased risk of identity theft and fraud due to her financial and personal information being sold on the Internet black market and/or misused by criminals.

39. Plaintiff John A. Thomas, II, is a customer of Defendants. When becoming a customer of Defendants, Mr. Thomas provided Defendants with sensitive personal and/or financial information. He reasonably believed Defendants would maintain this personal and/or financial information in a secure manner and provided his information to Defendants on that basis. Had Mr. Thomas known that Defendants would not maintain his information in a reasonably secure manner, he would not have provided that information to Defendants.

40. Mr. Thomas's personal information was compromised in and as a result of the Anthem data breach. Mr. Thomas was harmed by having his financial and/or personal information compromised and faces the imminent threat of future additional harm from the increased risk of identity theft and fraud due to his financial and personal information being sold on the Internet black market and/or misused by criminals.

### **CLASS ACTION ALLEGATIONS**

41. Pursuant to Federal Rule 23, Plaintiffs bring their claims that Defendants violated state data breach statutes (Count I) on behalf of separate state classes in and under the respective data breach statutes of the states of California, Colorado, Connecticut, Georgia, Kentucky, Virginia, and Wisconsin. These classes are defined as follows:

#### **State Data Breach Statute Classes:**

All residents of [name of State] whose personal information was compromised as a result of the Anthem data breach first publicly reported on February 4, 2015.

42. Pursuant to Federal Rule 23, Plaintiffs bring separate claims for negligence (Count II), breach of contract and implied contract (Count III), and bailment (Count IV) on behalf of the respective state classes in and under the laws

of each respective State of the United States as set forth in Counts II, III, and IV.

These classes for each of the foregoing claims are defined as follows:

**State [Negligence, Breach of Contract and Implied Contract, or Bailment] Class:**

All residents of [name of State] whose personal information was compromised as a result of the Anthem data breach first publicly reported on February 4, 2015.

43. Excluded from each of the above Classes are Anthem, including any entity in which Anthem has a controlling interest or is a parent or subsidiary, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Anthem. This includes Blue Cross. Also excluded are the judges and court personnel in this case and any members of their immediate families.

44. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of the claims on a class-wide basis using the same exclusive and common evidence as would be used to prove those elements in individual actions alleging the same claims.

45. All members of the purposed Classes are readily ascertainable. Anthem has access to addresses and other contact information for millions of members of the Classes, which can be used for providing notice to many Class members.

46. **Numerosity.** Plaintiffs do not know the exact number of Class members but believe that the Class comprises millions of consumers throughout these United States. As such, Class members are so numerous that joinder of all members is impracticable.

47. **Commonality and predominance.** Well-defined, nearly identical legal or factual questions affect all Class members. These questions predominate over questions that might affect individual Class members. These common questions include, but are not limited to, the following:

- a. Whether there was an unauthorized disclosure by Defendants of Class members' personal and/or financial information;
- b. Whether Defendants enabled an unauthorized disclosure of Class members' personal and/or financial information;
- c. Whether Defendants misrepresented the safety and security of Class members' personal and/or financial information maintained by Defendants;
- d. Whether Defendants implemented and maintained reasonable procedures and practices appropriate for maintaining the safety and security of Class members' personal and/or financial information;

- e. When Defendants became aware of an unauthorized disclosure of Class members' personal and/or financial information;
- f. Whether Defendants unreasonably delayed notifying Class members of an unauthorized disclosure of Class members' personal and/or financial information;
- g. Whether Defendants intentionally delayed notifying Class members of an unauthorized disclosure of Class members' personal and/or financial information;
- h. Whether Defendants' conduct was negligent;
- i. Whether Defendants' conduct was deceptive;
- j. Whether Defendants' conduct was knowing, willful, intentional, and/or malicious;
- k. Whether Plaintiffs and the Class are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

48. **Typicality.** Plaintiffs' claims are typical of the claims of the Class. Plaintiffs and all Class members were injured through Anthem's misconduct described above and assert the same claims for relief. The same events and conduct that give rise to Plaintiffs' claims are identical to those that give rise to the claims of every other Class member because each Plaintiff and Class member is a

person that has suffered harm as a direct result of the same conduct (and omissions of material facts) engaged in by Defendants and resulting in the Anthem data breach.

49. **Adequacy.** Plaintiffs will fairly and adequately protect Class members' interests. Plaintiffs have no interests antagonistic to Class members' interests, and Plaintiffs have retained counsel that has considerable experience and success in prosecuting complex class action and consumer protection cases.

50. **Superiority.** A class action is superior to all other available methods for fairly and efficiently adjudicating the claims of Plaintiffs and the Class members. Plaintiffs and the Class members have been harmed by Anthem's wrongful actions and inaction. Litigating this case as a class action will reduce the possibility of repetitious litigation relating to Anthem's wrongful actions and inaction.

51. A class action is an appropriate method for the fair and efficient adjudication of this controversy. There is no special interest in the members of the Class individually controlling the prosecution of separate actions. The loss of money and other harm sustained by many individual Class members will not be large enough to justify individual actions, especially in proportion to the significant costs and expenses necessary to prosecute this action. The expense and burden of

individual litigation makes it impossible for many members of the Class individually to address the wrongs done to them. Class treatment will permit the adjudication of claims of Class members who could not afford individually to litigate their claims against Defendants. Class treatment will permit a large number of similarly situated persons to prosecute their common claims in a single form simultaneously, efficiently, and without duplication of effort and expense that numerous individual actions would entail. No difficulties are likely to be encountered in the management of this class action that would preclude its maintenance as a class action, and no superior alternative exists for the fair and efficient adjudication of this controversy. Furthermore, Anthem and Blue Cross transact substantial business in Georgia. Anthem will not be prejudiced or inconvenienced by the maintenance of this class action in this forum.

52. Class certification, therefore, is appropriate under Federal Rules 23(a) and (b)(3). The above common questions of law or fact predominate over any questions affecting individual members of the Classes, and a class action is superior to other available methods for the fair and efficient adjudication of the controversy.

53. Class certification is also appropriate under Federal Rules 23(a) and (b)(2), because Defendants have acted or have refused to act on grounds generally

applicable to the Classes, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Classes as a whole.

54. The expense and burden of litigation will substantially impair the ability of Plaintiffs and Class members to pursue individual lawsuits to vindicate their rights. Absent a class action, Defendants will retain the benefits of their wrongdoing despite serious violations of the law.

**COUNT I**

**VIOLATIONS OF STATE DATA BREACH STATUTES**  
**(On behalf of Plaintiffs and the State Data Breach Statute Classes.)**

55. Plaintiffs reallege and incorporate by reference every allegation set forth in the preceding paragraphs as though alleged in this Count.

56. Legislatures in the states and jurisdictions listed below have enacted data breach statutes. These statutes generally require that any person or business conducting business within the state that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system to any resident of the state whose personal information was acquired by an unauthorized person, and further require that the disclosure of the breach be made in the most expedient time possible and without unreasonable delay.

57. The Anthem data breach constitutes a breach of the security system of Anthem within the meaning of the below state data breach statutes and the data breached is protected and covered by the below data breach statutes.

58. Plaintiffs' and Class members' names, birthdates, email addresses, employment details, social security numbers, and street addresses constitute personal information under and subject to the below state data breach statutes.

59. Anthem and Blue Cross unreasonably delayed in informing the public, including Plaintiffs and members of the State Data Breach Statute Classes (collectively, "Class," as used in this Count I), about the breach of security of Plaintiffs' and Class members' confidential and non-public personal information after Anthem knew or should have known that the data breach had occurred.

60. Anthem and Blue Cross failed to disclose to Plaintiffs and Class members without unreasonable delay and in the most expedient time possible, the breach of security of Plaintiffs' and Class members' personal and financial information when Defendants knew or reasonably believed such information had been compromised.

61. Plaintiffs and members of the Class suffered harm directly resulting from Anthem's failure to provide and the delay in providing Plaintiffs and Class members with timely and accurate notice as required by the below state data

breach statutes. Plaintiffs suffered the damages alleged above as a direct result of Anthem's delay in providing timely and accurate notice of the data breach.

62. Had Defendants provided timely and accurate notice of the Anthem data breach, Plaintiffs and Class members would have been able to avoid and/or attempt to ameliorate or mitigate the damages and harm resulting in the unreasonable delay by Defendants in providing notice.

63. Anthem's failure to provide timely and accurate notice of the Anthem data breach violated the following state data breach statutes where Defendants do substantial business:

- a. Cal. Civ. Code § 1798.83(a), et seq.;
- b. Colo. Rev. Stat. Ann § 6-1-716(2), et seq.;
- c. Conn. Gen. Stat. Ann. § 36a-701b(b), et seq.;
- d. Ga. Code Ann. § 10-1-912(a), et seq.;
- e. Ky. Rev. Stat. Ann. § 365.732(2), et seq.;
- f. Va. Code. Ann. § 18.2-186.6(B), et seq.; and
- g. Wis. Stat. Ann. § 134.98(2), et seq.

64. Plaintiffs and members of each of the State Data Breach Statute Classes seek all remedies available under their respective state data breach statutes, including but not limited to a) damages suffered by Plaintiffs and Class members

as alleged above, b) equitable relief, including injunctive relief, and c) reasonable attorney fees and costs, as provided by law.

**COUNT II**

**NEGLIGENCE**

**(On behalf of Plaintiffs and the separate State Negligence Classes.)**

65. Plaintiffs reallege and incorporate by reference every allegation set forth in the preceding paragraphs as though alleged in this Count.

66. Defendants came into possession, custody, and/or control of personal and/or financial information of Plaintiffs and Class members.

67. Defendants owed a duty to Plaintiffs and members of the State Negligence Classes (collectively, “Class” as used in this Count II) to exercise reasonable care in safeguarding and securing the personal and/or financial information of Plaintiffs and Class members in their possession, custody, and/or control.

68. Defendants had a duty to exercise reasonable care in implementing and maintaining reasonable procedures and practices appropriate for maintaining the safety and security of Plaintiffs’ and Class members’ personal and/or financial information in their possession, custody, and/or control.

69. Defendants had a duty to exercise reasonable care in timely notifying Plaintiffs and Class members of an unauthorized disclosure of Plaintiffs’ and Class

members' personal and/or financial information in their possession, custody, and/or control.

70. Defendants, through their actions and/or omissions, unlawfully breached their duty to Plaintiffs and Class members by failing to exercise reasonable care in safeguarding and securing the personal and/or financial information of Plaintiffs and Class members in their possession, custody, and/or control.

71. Defendants, through their actions and/or omissions, unlawfully breached their duty to Plaintiffs and Class members by failing to exercise reasonable care in implementing and maintaining reasonable procedures and practices appropriate for maintaining the safety and security of Plaintiffs' and Class members' personal and/or financial information in their possession, custody, and/or control.

72. Defendants, through their actions and/or omissions, unlawfully breached their duty to Plaintiffs and Class members by failing to exercise reasonable care in timely notifying Plaintiffs and Class members of an unauthorized disclosure of Plaintiffs' and Class members' personal and/or financial information in their possession, custody, and/or control.

73. Defendants' negligent and wrongful breach of duties owed to Plaintiffs and Class members proximately caused an unauthorized disclosure of Plaintiffs' and Class members' personal and/or financial information in their possession, custody, and/or control.

74. As a direct and proximate result of Anthem's negligent conduct, Plaintiffs and the Class have suffered injury and are entitled to damages in an amount to be proven at trial.

**COUNT III**

**BREACH OF CONTRACT AND IMPLIED CONTRACT**  
**(On behalf of Plaintiffs and the State Breach of Contract and Implied Contract Classes.)**

75. Plaintiffs reallege and incorporate by reference every allegation set forth in the preceding paragraphs as though alleged in this Count.

76. When Plaintiffs and members of the State Breach of Contract and Implied Contract Classes (collectively, "Class" as used in this Count III) provided their personal information to Defendants in order to enroll in insurance policies of Defendants, Plaintiffs and members of the Class entered into contracts and implied contracts with Defendants pursuant to which Defendants agreed to safeguard and protect such information and to timely and accurately notify Plaintiffs and Class

members that their data had been breached and compromised. For example, the Blue Cross contract assures customers as follows:

- Blue Cross and Blue Shield of Georgia is committed to protecting the confidentiality of Social Security numbers and other Personal Information.
- Blue Cross and Blue Shield of Georgia's Privacy Policy imposes a number of standards to:
  - guard the confidentiality of Social Security numbers and other personal information,
  - prohibit the unlawful disclosure of Social Security numbers, and
  - limit access to Social Security numbers.

The contract further provides:

Blue Cross and Blue Shield of Georgia safeguards Social Security numbers and other personal information by having physical, technical, and administrative safeguards in place.

77. Defendants solicited and invited Plaintiffs and members of the Class to enroll in insurance policies and programs with Defendants. Plaintiffs and members of the Class accepted Anthem's offers and provided the requested information to purchase insurance from Defendants.

78. Each enrollment or application made by Plaintiffs and members of the Class with Defendants was made pursuant to the mutually agreed upon contract and further implied contractual provisions under which Defendants agreed to safeguard and protect Plaintiffs' and Class members' personal and financial information, and to timely and accurately notify them that such information was compromised and breached.

79. Plaintiffs and Class members would not have provided and entrusted their financial and personal information to Defendants in order to enroll in insurance with Defendants in the absence of the contractual and implied contractual protections between them and Defendants.

80. Plaintiffs and members of the Class fully performed their obligations under the contracts and implied contracts with Defendants.

81. Defendants breached the contracts and implied contracts they made with Plaintiffs and Class members by failing to safeguard and protect the personal and financial information of Plaintiffs and members of the Class and by failing to provide timely and accurate notice to them that their personal and financial information was compromised in and as a result of the data breach.

82. The losses and damages sustained by Plaintiffs and Class members as described herein were the direct and proximate result of Defendants' breaches of contract or implied contract.

83. Wherefore, Plaintiffs pray for relief as set forth below.

**COUNT IV**

**BAILMENT**

**(On behalf of Plaintiffs and the separate State Bailment Classes.)**

84. Plaintiffs reallege and incorporate by reference every allegation set forth in the preceding paragraphs as though alleged in this Count.

85. Plaintiffs and members of the separate State Bailment Classes (collectively, “Class” as used in this Count IV) delivered their personal and financial information, to Defendants for the exclusive purpose of enrolling in insurance policies and/or purchasing insurance from Defendants.

86. In delivering their personal and financial information to Defendants, Plaintiffs and Class members intended and understood that Defendants would adequately safeguard their personal and financial information.

87. Defendants accepted possession of Plaintiffs’ and Class members’ personal and financial information for the purpose of purchasing insurance from Defendants by Plaintiffs and members of the Class.

88. By accepting possession of Plaintiffs’ and Class members’ personal and financial information, Defendants understood that Plaintiffs and Class members expected Defendants to adequately safeguard their personal and financial information. Accordingly, a bailment (or deposit) was established for the mutual benefit of the parties.

89. During the bailment (or deposit), Defendants owed a duty to Plaintiffs and Class members to exercise reasonable care, diligence, and prudence in protecting their personal and financial information.

90. Defendants breached their duty of care by failing to take appropriate measures to safeguard and protect Plaintiffs' and Class members' personal and financial information, resulting in the unlawful and unauthorized access to and misuse of Plaintiffs' and Class members' personal and financial information.

91. Defendants further breached their duty to safeguard Plaintiffs' and Class members' personal and financial information by failing to timely and accurately notify them that their information had been compromised as a result of the data breach.

92. Defendants failed to return, purge, or delete the personal and financial information of Plaintiffs and members of the Class at the conclusion of the bailment (or deposit) and within the time limits allowed by law.

93. As a direct and proximate result of Defendants' breach of their duty, Plaintiffs and Class members suffered consequential damages that were reasonably foreseeable, including but not limited to the damages set forth above.

94. As a direct and proximate result of Defendants' breach of their duty, the personal and financial information of Plaintiffs and Class members entrusted to Defendants during the bailment (or deposit) was damaged and its value diminished.

95. Wherefore, Plaintiffs pray for relief as set forth below.

**PRAYER FOR RELIEF**

On behalf of themselves and the Classes set forth above, Plaintiffs request the Court order relief and enter judgment against Defendants and enter an order:

- A. certifying this case as a class action pursuant to Federal Rules 23(a), (b)(2), and (b)(3), and, pursuant to Federal Rule 23(g), appoint the named Plaintiffs to be Class representatives and their undersigned counsel to be Class counsel;
- B. requiring Defendants to make whole any losses suffered by Plaintiffs and Class members;
- C. enjoining Defendants from further engaging in the unlawful conduct complained of herein;
- D. awarding Plaintiffs and the Classes appropriate relief, including actual and statutory damages, restitution, and disgorgement;
- E. awarding pre-judgment and post-judgment interest;
- F. requiring Defendants to pay for notifying the Class of the pendency of this action;
- G. establishing a fluid recovery fund for distribution of unclaimed funds;
- H. requiring Defendants to pay Plaintiffs and Class members reasonable attorneys' fees, expenses, and the costs of this action; and

I. providing all other and further relief as this Court deems necessary, just, and proper.

**DEMAND FOR TRIAL BY JURY**

Plaintiffs demand a trial by jury on all issues so triable.

DATED this 5th day of February, 2015.

Respectfully submitted,

BY: WEBB, KLASE & LEMOND, LLC

/s/ E. Adam Webb

E. Adam Webb  
Georgia State Bar No. 743910  
Matthew C. Klase  
Georgia State Bar No. 141903  
G. Franklin Lemond, Jr.  
Georgia State Bar No. 141315

1900 The Exchange, S.E.  
Suite 480  
Atlanta, Georgia 30339  
(770) 444-9325  
(770) 217-9950 (fax)  
Adam@WebbLLC.com  
Matt@WebbLLC.com  
Franklin@WebbLLC.com

Attorneys for Plaintiffs